GDPR
General Data Protection Regulation

Make sure you have everything in place to protect your corporate data and prevent data leaks.

The General Data Protection Regulation is a hot topic. Everywhere you'll find information and seminaries of what, where, how and especially, when. Fundamentally, the new GDPR regulation is a mainly legal story, a bunch of regulations which need to be in place by May 2018.

In an effort to assist you with your preparations, this document is designed as a quick guide to assemble a set of tools that completes your GDPR story. In no case this can be considered as a complete GDPR solution, but will focus on some of the legislation's fundamentals and on IT-related security precautions you can take.

What is GDPR?

GDPR (General Data Protection Regulation) is a set of rules delivered by the European Commission, that enables people to have better control over their personal data. The key objective is that every person should be able to get a hold of its personal data such as addresses, telephone numbers as well as medical information.

Who does GDPR apply to?

In today's digital economy, personal data has acquired enormous economic significance, in particular in the area of big data. By unifying Europe's rules on data protection, lawmakers are creating a business opportunity and encouraging innovation.

Therefore, every European company or company that performs business in the E.U. that stores any kind of personal information that makes it able to track an individual, must comply to GDPR regulations.

How do the GDPR rules affect my business?

1. The general guideline is that before stocking the information of an individual, the company needs to inform that individual that it will keep, what it will keep and what it will do with the person's personal data. Even more, no data may be kept on file if the company has no reason to store that specific information.

   For example, a company cannot store the weight of somebody if they sell books, since there is no logical relation between the two.

2. Secondly, all stored information must stay up to date at all times, this implies that every change in address or phone number must be modified in the database immediately upon reception of the information.

3. Thirdly, people have the right to demand a data transfer of all personal information towards another company. For example, if an individual changes telecom providers, both the old and the new provider need to work together to exchange the individual's information.

EASIER ACCESS TO YOUR OWN DATA

Individuals will have more information on how their data is processed in a clear and understandable way

A RIGHT TO DATA PORTABILITY

It will be easier to transfer your personal data between service providers

Kappa Data

THE ART OF
IT INFRASTRUCTURE AND SECURITY DISTRIBUTION

4 A more challenging rule, is the right to be forgotten. If a person requests to eliminate all of the information that is stored about him/her, the company is obligated to delete everything on that person from all of the company's storage carriers and lists. Including all databases, backups etc. that the company has created.

5 The final and most important new rule is that a company needs to report every data leak to the public. This implies that when your website or data storage center is hacked and the hacker was able to access a database with email addresses or personal information, this leak must be reported within 72 hours.

Do I need a Data Protection Officer?

The need for a dedicated Data Protection Officer (DPO) applies for all EU and non-EU companies and is applicable to companies that sell goods and services or regularly monitor Europeans or process data on them at certain levels.

If data is your business and if you employ more than 250 people you are required to appoint and educate an official DPO or work with one on a contract basis.

What if you're not compliant?

If you fail to comply to this regulation, you risk a heavy penalty. This penalty can amount to 4 percent of your world-wide wide revenue with a maximum of 20 million euro.

Thus, concluding this brief GDPR-regulatory summary. Quite possibly, there are still questions and ambiguities that remain, even in the legislation, but only time can resolve these. However, at Kappa Data we aim to inform you as good as we can and therefore encourage you to act on the GDPR regulation. As we believe that investing in protection is something that all companies need to do, regardless of legal requirements such as GDPR.

You can find an overview of the solutions in our portfolio that may help you to complete your GDPR toolkit here below and, if you haven't done so yet, we kindly encourage you to consult a jurist to accompany you in your GDPR compliancy journey.

Main Sources:

www.europa.eu

www.eudataprotectionregulation.com

www.pwc.com

A CLARIFIED "RIGHT TO BE FORGOTTEN"

When you no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted.

THE RIGHT TO KNOW WHEN YOUR DATA HAS BEEN HACKED

For example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures.

YOUR PREFERRED IT SECURITY PARTNER

Kappa Data

THE ART OF

IT INFRASTRUCTURE AND SECURITY DISTRIBUTION

GDPR
General Data Protection Regulation

SOLUTIONS

PULSE SECURE

Pulse Workspace is a Mobile Device Management solution that manages IOS and Android devices, no matter if they are corporate, owned or private. Upon rollout, some kind of sandbox is installed on the device that separates private data from corporate data. No communication is possible between those two environments. If the user leaves the company or the device is stolen/lost, then you can wipe the whole sandbox without touching the private data.

Pulse Connect Secure and Pulse Policy Secure will act as a gateway for both internal and external users to make sure you have control over not only who accesses the network, but if the devices are compliant with all necessary regulations (drive encryption, anti-virus, updates, …). You can even enforce settings in the browser e.g. “do not store passwords”.

VASCO

In addition to remote access solutions or to application security, you need to consider two factor authentication. There is no need to explain how easy passwords are guessed or stolen, but there is a need to explain the consequences related to GDPR. If data leaked because a user was sloppy and someone got a hold on his password, it is the company that pays the bill of the data leak.

By using dual factor authentication such as OTP (one time password), fingerprints or QR-codes, ordinary passwords become totally unusable when leaked.

STORMSHIELD

Unfortunately it is not always an option to keep all data inside a company. You may need to send it via email, transport it via USB or put it on a cloud drive. Once this is done, you can never 100% control who has access to these confidential files.

However, thanks to Shormshield Data Security, you can protect what is in that file by using encryption and access security. Only the people invited by the owner of the file, can decrypt the file and read it’s content.

Pulse Secure

VASCO
TRUST FOR THE DIGITAL WORLD

STORMSHIELD

Kappa Data
THE ART OF
IT INFRASTRUCTURE AND SECURITY DISTRIBUTION

TREND MICRO

The advantage of Trend Micro is that they play on multiple layers in the network so they can apply security measures on all levels. Like Stormshield they can encrypt your data, and they can even do more. Trend Micro can block access to USB drives. They can recognize patterns in DATA that is sent out and block or replace confidential information. (DLP)

Through the use of email reputation services and web reputation services users are protected from phishing mails and sites. A threath like this could be the first step in giving remote control or unintentionally sharing passwords.

Office 365 users have different security challenges. In fact, the data is already outside the company. Therefore, Trend Micro has installed a security center inside the datacenters of Microsoft. That way they can protect all data that is in Office 365 from the inside-out. This implies the ability for DLP within email, SharePoint and OneDrive.

With DLP, the integrity monitoring tool can alert you when changes happen to the key operating system and application files, as well as unwanted modifications on essential processes and ports.

BARRACUDA

The Barracuda Web Application Firewall protects you against attacks on your webshop or other public services. You may have the latest fixes on the underlying operating system; you may have written the most secure code, but you may not have had the time to install the latest fix that just came out for your content management system. Meanwhile you are vulnerable. The BCD WAF scans your site and automatically implements all necessary security updates. It provides you with all the time that you need to install missing updates.

The WAF is placed at the ideal position in your network to capture information leaks and (partially) replace them with dummy information (DLP).

Knowing what kind of server you are running, is essential information for a hacker to prepare himself for a future attack. Lots of information is offered on a plate by default, simply in the HTML source code. The Barracuda WAF will cut out this information and make it impossible for a hacker to trace this server information.

A second solution, the Email Security Gateway, can be used to inspect outgoing mails and apply DLP policies to protect confidential data.

JUNIPER

Where malware could be a cause for leaks in the network, Juniper is capable to isolate an infected host from the network to make sure no cross infection nor data leakage is possible. This solution makes part of a complete story which is called SDSN (Software Defined Secure Networking). Sky ATP is the SDSN tool for ransomware checks that always delivers up to date cloud based protection.

You need to protect the network from attacks and make sure no data leaves the network. But if it does, then you'll need to know this. A Security Information and Event Management System covers this part. The Juniper JSA series is a complete SIEM solution built on IBM's QRadar proven technology. It monitors the complete network and gives a holistic view of all events and issues that would otherwise remain unnoticed.

TREND MICRO

Barracuda

JUNIPER NETWORKS

Kappa Data

THE ART OF
IT INFRASTRUCTURE AND SECURITY DISTRIBUTION